Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (original) A security system comprising a network,

said network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a hardware processor providing transport layer protocol processing,

said hardware processor comprising

a protocol processing engine to do transport layer protocol processing; or

a programmable rule processing engine to analyze network traffic for rule matching or taking actions on matched rules or a combination thereof; or

a security processing engine to do encryption, decryption, authorization or

authentication or a combination thereof using standard or proprietary security protocols; or

a packet classification engine to classify the network traffic; or

a packet processing engine to perform packet processing tasks; or

a combination of any of the foregoing,

said security system providing multiple protocol layer security in said network.

2. (original) A security system for a storage area network,

said storage area network comprising one or more networked systems of one or more types,

said security system comprising a set of systems from said one or more networked systems,

a plurality of said set of systems comprising a. hardware processor providing transport layer protocol processing,

said hardware processor comprising

a storage protocol processing engine to do protocol processing; or

a protocol processing engine to do transport layer protocol processing; or

a programmable rule processing engine to analyze storage area network traffic for rule matching or taking actions on matched rules or a combination thereof; or

a security processing engine to do encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols; or

a packet classification engine to classify the storage area network traffic; or

a packet processing engine to perform packet processing tasks like header processing or deep packet processing or a combination thereof; or

a combination of any or the foregoing,

said security system providing multiple protocol layer security in said storage area network.

3. (original) The security system of claim 1 further comprising:

a. at least one central manager for compiling and distributing security rules; and

b. at least one security policy driver to communicate with the central manager and to set up rules in said hardware processor on at least one of said plurality of said one or more networked systems to analyze and enforce security based on said rules.

4. (original) The security system of claim 3 wherein the central manager comprises at least one of:

a. A Security Policy Developer Interface for entering security policy;

b. A Security Rules Compiler for compiling security policies into rules;

c. A Rules Distribution Engine to distributed rules to said plurality of said one or more networked systems;

d. A Security Policy Manager Interface to manage said plurality of said one or more networked systems;

e. A Security Monitoring Engine to monitor said network;

f. An event collection/management engine to manage said network and collect events or reports from at least one of said plurality of said one or more networked systems; or

g. a combination of any of the foregoing.

5. (original) The security system of claim 3 wherein at least one of said networked systems provides security based on rules for

a. OSI protocol layer two to provide layer two or MAC layer filtering; or

b. OSI protocol layer three to provide layer three or network layer filtering; or

c. OSI protocol layer four to provide layer four or transport layer filtering; or

d. OSI protocol layers five through seven to provide upper layer or application layer filtering; or

e. a combination of any of the foregoing.

6. (original) The security system of claim 1 including security protocols comprising at least one of IPSEC, OPSEC, SSL, TLS, AES, DES, 3DES, SHA1, MD4, MD5, RSA, CHAP, Kerberos, a proprietary protocol, or a combination of any of the foregoing.

7. (original) The security system of claim 3 wherein at least one of the at least one policy drivers executes on a processor of said hardware processor or on a host processor of at least one of said networked systems.

8. (original) The security system of claim 1 including multiple protocol layer security that includes security functions performed at one or more protocol layers of the OSI stack to provide packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or a combination of any of the foregoing.

9. (original) A security system comprising a network,

said network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a hardware processor providing remote direct memory access capability,

said hardware processor comprising

an RDMA mechanism for performing RDMA data transfer or

a protocol processing engine to do transport layer protocol processing; or

a programmable rule processing engine to analyze network traffic for rule matching or taking actions on matched rules or a combination thereof; or

a security processing engine to do encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols; or

a packet classification engine to classify the network traffic; or

a packet processing engine to perform packet processing tasks like header processing or deep packet processing or a combination thereof; or

a combination of any of the foregoing,

said security system providing multiple protocol layer security in said network.

10. (original) The security system of claim 9 where said hardware processor provides a transport layer remote direct memory access capability.

11. (original) The security system of claim 9 further comprising:

a. at least one central manager for compiling and distributing security rules; and

b. at least one security policy driver to communicate with the central manager to set up rules in said hardware processor on at least one of said plurality of said one or more networked systems to analyze and enforce security based on said rules.

12. (original) The security system of claim 11 wherein the central manager comprises at least one of:

a. A Security Policy Developer Interface for entering security policy;

b. A Security Rules Compiler for compiling security policies into rules;

c. A Rules Distribution Engine to distribute rules to said plurality of said one or more networked systems

d. A Security Policy Manager Interface to manage said plurality of said one or more networked systems;

e. A Security Monitoring Engine to monitor said network;

f. An event collection/management engine to manage said network and collect events or reports from said plurality of said one or more networked systems; or

g. a combination of any of the foregoing.

13. (original) The security system of claim 11 wherein at least one of said networked systems provides security based on rules for

a. OSI protocol layer two to provide layer two or MAC layer filtering; or

b. OSI protocol layer three to provide layer three or network layer filtering; or

c. OSI protocol layer four to provide layer four or transport layer filtering; or

d. OSI protocol layers five through seven to provide upper layer or application layer filtering; or

e. a combination of any of the foregoing.

14. (original) The security system of claim 9 including security protocols comprising at least one of IPSEC, OPSEC, SSL, TLS, AES, DES, 3DES, SHA1, MD4, MD5, RSA, CHAP, Kerberos, a proprietary protocol or a combination of any of the foregoing.

15. (original) The security system of claim 11 wherein at least one of the at least one policy driver that executes on a processor of said hardware processor or on a host processor of at least one of said networked systems.

16. (original) The security system of claim 9 including multiple protocol layer security that includes security functions performed at one or more protocol layers of the OSI stack to provide packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or a combination of any of the foregoing.

17. (original) The combination of claim 1 wherein said one or more networked systems comprises a blade server, thin server, media server, streaming media server, appliance server, Unix server, Linux server, Windows or Windows derivative server, AIX server, clustered server, database server, grid computing server, VOIP server, wireless gateway server, security server, file server, network attached storage server, game server, router, switch, wireless access point, workstation, desktop computer, notebook computer, laptop computer, utility computing system or gateway device or a combination of any of the foregoing.

18. (original) The combination of claim 9 wherein said one or more networked systems comprises a blade server, thin server, media server, streaming media server, appliance server, Unix server, Linux server, Windows or Windows derivative server, AIX server, clustered server, database server, grid computing server, VOIP server, wireless gateway server, security server, file server, network attached storage server, game server, router, switch, wireless access point, workstation, desktop computer, notebook computer, laptop computer, utility computing system or gateway device or a combination of any of the foregoing.

19. (original) The security system of claim 1 wherein said packet processing steps include header processing or deep packet processing or a combination thereof.

20. (original) The security system of claim 2 further comprising:

a. at least one central manager for compiling and distributing storage area network security rules; and

b. at least one security policy driver to communicate with the central manager to set up rules in said hardware processor on at least one of said plurality of said one or more networked systems to analyze and enforce storage area network security based on said rules.

21. (original) The security system of claim 20 wherein the central manager comprises at least one of:

a. A Security Policy Developer Interface for entering security policy;

b. A Security Rules Compiler for compiling security policies into rules;

c. A Rules Distribution Engine to distribute rules to the said plurality of said one or more networked systems

d. A Security Policy Manager Interface to manage said plurality of said one or more networked systems;

e. A Security Monitoring Engine to monitor said network;

f. An event collection/management engine to manage said network and collect events or reports from said plurality of said one or more networked systems; or

g. a combination of any of the foregoing.

22. (original) The security system of claim 20 wherein at least one of said networked systems provides security based on rules for

a. OSI protocol layer two to provide layer two or MAC layer filtering; or

b. OSI protocol layer three to provide layer three or network layer filtering; or

c. OSI protocol layer four to provide layer four or transport layer filtering; or

d. OSI protocol layers five through seven to provide upper layer or application layer filtering; or

e. Storage protocol layer to provide storage protocol layer filtering; or

f. a combination of any of the foregoing.

23. (original) The security system of claim 2 including security protocols comprising at least one of IPSEC, OPSEC, SSL, TLS, AES, DES, 3DES, SHA1, MD4, MD5, RSA, CHAP, Kerberos, a proprietary protocol or a combination of any of the foregoing.

24. (original) The security system of claim 20 including a policy driver that executes on a processor of said hardware processor or on a host processor of at least one of said networked systems.

25. (original) The security system of claim 2 including multiple protocol layer security that includes security functions performed at one or more protocol layers of the OSI stack to provide packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or a combination of any of the foregoing.

26. (original) A security system for a network,

said network comprising one or more networked systems of one or more types,

said security system comprising a set of systems from said one or more networked systems,

a plurality of said set of systems comprising a hardware processor providing transport layer protocol processing,

said hardware processor comprising

a protocol processing engine to do transport layer protocol processing; or

a programmable rule processing engine to analyze network traffic for rule matching or taking actions on matched rules or a combination thereof; or

a security processing engine to do encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols; or

a packet classification engine to classify the network traffic; or

a packet processing engine to perform packet processing tasks like header processing or deep packet processing or a combination thereof; or

a combination of the foregoing,

said security system providing multiple protocol layer security in said network.

27. (original) A security system for a network comprising one or more networked systems, at least one of said networked systems having a hardware processor providing a protocol processing stack, said security system providing a secure operating environment for said protocol processing stack for trusted computing needs of one or more of said networked systems by providing a policy driver for setting up the hardware processor for security policy rules to be enforced by said hardware processor, and a central manager for compiling and distributing said rules and monitoring the enforcement of said rules by said hardware processor.

28. (new) A security system comprising a network,

said network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a hardware processor providing transport layer protocol processing,

said hardware processor comprising

a protocol processing engine for performing transport layer protocol processing;

said security system providing multiple protocol layer security in said network.

29. (new) The hardware processor of claim 28 further comprising:

a programmable rule processing engine for analyzing network traffic for security rule matching or taking actions on matched rules or a combination thereof;

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

a packet classification engine for classifying the network traffic; or

a packet processing engine for performing packet processing tasks

or a combination of the foregoing.

30. (new) The hardware processor of claim 29 wherein said packet processing tasks comprise header processing, deep packet processing or a combination thereof.

31. (new) A security system for a storage area network,

said storage area network comprising one or more networked systems of one or more types,

said security system comprising a set of systems from said one or more networked systems,

a plurality of said set of systems comprising a hardware processor providing transport layer protocol processing,

said hardware processor comprising

a protocol processing engine for performing transport layer protocol processing;

said security system providing multiple protocol layer security in said storage area network.

32. (new) The hardware processor of claim 31 further comprising:

a storage protocol processing engine for performing storage protocol processing;

a programmable rule processing engine for analyzing storage area network traffic for security rule matching or taking actions on matched rules or a combination thereof;

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

a packet classification engine for classifying the storage area network traffic; or

a packet processing engine for performing packet processing tasks

or a combination of the foregoing.

33. (new) The security system of claim 28 comprising multiple protocol layer security that comprises security functions performed at one or more protocol layers of an OSI stack for providing packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or detect other security attacks or a combination of any of the foregoing.

34. (new) A security system comprising a network,

said network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a hardware processor providing remote direct memory access capability,

said hardware processor comprising

an RDMA mechanism for performing RDMA data transfer

said security system providing multiple protocol layer security in said network.

35. (new) The hardware processor of claim 34 further comprising:

a protocol processing engine for performing transport layer protocol processing;

a programmable rule processing engine for analyzing network traffic for security rule matching or taking actions on matched rules or a combination thereof;

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

a packet classification engine for classifying the network traffic; or

a packet processing engine for performing packet processing tasks.

or a combination of the foregoing.

36. (new) The hardware processor of claim 35 wherein said packet processing comprises header processing, deep packet processing or a combination thereof.

37. (new) The security system of claim 34 where said hardware processor provides a transport layer remote direct memory access capability.

38. (new) The security system of claim 34 comprising multiple protocol layer security that comprises security functions performed at one or more protocol layers of the OSI stack for providing packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or detect other security attacks or a combination of any of the foregoing.

39. (new) The security system of claim 31 comprising multiple protocol layer security that comprises security functions performed at one or more protocol layers of the OSI stack for providing packet filtering, intrusion detection, denial of service attack detection, port scanning detection, virus scan, spam filtering, unauthorized access, or detect other security attacks or a combination of any of the foregoing.

40. (new) A security system comprising a network,

said network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a remote direct memory access capability for performing RDMA data transfers

said security system providing multiple protocol layer security in said network.

41. (new) The remote direct memory access capability of claim 40 comprising a hardware processor, said hardware processor comprising an RDMA mechanism for performing RDMA data transfers.

42. (new) The remote direct memory access capability of claim 40 comprising a hardware processor, said hardware processor provides a transport layer remote direct memory access capability.

43. (new) The hardware processor of claim 41 further comprising:

a protocol processing engine for performing transport layer protocol processing;

a programmable rule processing engine for analyzing network traffic for security rule matching or taking actions on matched rules or a combination thereof;

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

a packet classification engine for classifying the network traffic; or

a packet processing engine for performing packet processing tasks.

or a combination of the foregoing.

44. (new) The hardware processor of claim 43 wherein said packet processing comprises header processing or deep packet processing or a combination thereof.

45. (new) A security system comprising a storage area network,

said storage area network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a remote direct memory access capability for performing RDMA data transfers

said security system providing multiple protocol layer security in said storage area network.

46. (new) The remote direct memory access capability of claim 45 comprising a hardware processor, said hardware processor comprising an RDMA mechanism for performing RDMA data transfers.

47. (new) The remote direct memory access capability of claim 45 comprising a hardware processor, said hardware processor provides a transport layer remote direct memory access capability.

48. (new) Said hardware processor of claim 46 further comprising

a storage protocol processing engine for performing storage protocol processing;

a protocol processing engine for performing transport layer protocol processing;

a programmable rule processing engine for analyzing storage area network traffic for security rule matching or taking actions on matched rules or a combination thereof;

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

a packet classification engine for classifying the storage area network traffic; or

a packet processing engine for performing packet processing tasks.

or a combination of the foregoing.

49. (new) The hardware processor of claim 48 wherein said packet processing comprises header processing, deep packet processing or a combination thereof.

50. (new) A security system comprising a network,

said network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a hardware processor providing transport layer protocol processing,

said hardware processor comprising

a protocol processing engine for performing transport layer protocol processing; and

a programmable rule processing engine for analyzing network traffic for security rule matching or taking actions on matched rules or a combination thereof;

said security system providing multiple protocol layer security in said network.

51. (new) A security system comprising a network,

said network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a hardware processor providing transport layer protocol processing,

said hardware processor comprising

a protocol processing engine for performing transport layer protocol processing;

a programmable rule processing engine for analyzing network traffic for security rule matching or taking actions on matched rules or a combination thereof; and

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

said security system providing multiple protocol layer security in said network.

52. (new) A security system for a storage area network,

said storage area network comprising one or more networked systems of one or more types,

said security system comprising a set of systems from said one or more networked systems,

a plurality of said set of systems comprising a hardware processor providing transport layer protocol processing,

said hardware processor comprising

a protocol processing engine for performing transport layer protocol processing; and

a storage protocol processing engine for performing storage protocol processing;

said security system providing multiple protocol layer security in said storage area network.

53. (new) The hardware processor of claim 52 further comprising:

a programmable rule processing engine for analyzing storage area network traffic for security rule matching or taking actions on matched rules or a combination thereof;

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

a packet classification engine for classifying the storage area network traffic; or

a packet processing engine for performing packet processing tasks.

or a combination of the foregoing.

54. (new) The hardware processor of claim 53 wherein said packet processing comprises header processing or deep packet processing or a combination thereof.

55. (new) A security system comprising a network,

said network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a hardware processor providing remote direct memory access capability,

said hardware processor comprising

an RDMA mechanism for performing RDMA data transfer and

a protocol processing engine for performing transport layer protocol processing;

said security system providing multiple protocol layer security in said network.

56. (new) The hardware processor of claim 55 further comprising:

a programmable rule processing engine for analyzing network traffic for security rule matching or taking actions on matched rules or a combination thereof;

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

a packet classification engine for classifying the network traffic; or

a packet processing engine for performing packet processing tasks.

or a combination of the foregoing.

57. (new) The hardware processor of claim 56 wherein said packet processing comprises. header processing or deep packet processing or a combination thereof.

58. (new) A security system for a storage area network,

said storage area network comprising one or more networked systems of one or more types,

a plurality of said one or more networked systems comprising a hardware processor providing remote direct memory access capability,

said hardware processor comprising

an RDMA mechanism for performing RDMA data transfer

said security system providing multiple protocol layer security in said storage area network.

59. (new) The hardware processor of claim 58 further comprising:

a storage protocol processing engine for performing storage protocol processing;

a protocol processing engine for performing transport layer protocol processing;

a programmable rule processing engine for analyzing network traffic for security rule matching or taking actions on matched rules or a combination thereof;

a security processing engine for performing encryption, decryption, authorization or authentication or a combination thereof using standard or proprietary security protocols;

a packet classification engine for classifying the network traffic; or

a packet processing engine to perform packet processing tasks

or a combination of the foregoing.

60. (new) The hardware processor of claim 59 wherein said packet processing comprises. header processing or deep packet processing or a combination thereof.

61. (new) The hardware processor of claim 32 wherein said packet processing tasks comprises

header processing or deep packet processing or a combination thereof.